CLAIMS

1. An apparatus, comprising:

inputs A, B and N, and an output S, the apparatus arranged to perform a modular operation, S=A.B mod N, the apparatus including a 2-stage Carry-Save Adder (2-CSA) and a 1-stage Carry-Save Adder (1-CSA), the 2-CSA arranged to receive 5 input signals:

U_0, being the partial product of N and Y_0;

U_1, being the subtraction of a previous version of S and U_6 wherein U_6 is either N or 0 depending on the value of the comparison between the result of the previous iteration and N;

U_2, being the partial product of B with the current version of A;

U_3, being S/2; and

U_4, being the carry output of the 1-CSA;

where result and carry outputs of the 2-CSA form two of three inputs to the 1-CSA, wherein the result (R) output of the 1-CSA is the desired result (S), and the third input to the 1-CSA is a compensation signal arranged to allow S to be calculated without knowing the constant J_0, where $J_0N<0> = -1.$ mod 2^p, where p is a block length into which A is sub-divided.

2. The apparatus of claim 1 wherein the compensation signal is generated to equal a delayed version of N in the event that t<p and the Result (R) output of the 2-CSA equals '1'.

3. The apparatus of claim 1 wherein the 2-CSA includes two 1-CSA arranged in series.

4. The apparatus of claim 1 wherein while processing bits 0 to p-1, register Y_0 is arranged such that the LSB of the Result (R) output of the 1-CSA is always ‘0’.

5. The apparatus of claim 1 wherein the apparatus is arranged to take the form of a custom integrated circuit.

6. The apparatus of claim 5 wherein the custom integrated circuit includes a digital signal processor (DSP).

7. An iterative method of performing a modular operation of S = A.B mod N, where A, B and N are encoded as multi-bit digital words, including the following steps:

a) setting S(-1) to 0, and i to 0;
b) setting S(i) to $(S(i-1) + A<i>B + NY_0)/2^p$;
c) setting S(i) to (S(i) - N) if $S(i) \geq N$; and
d) repeating steps b) and c) k times;

wherein:

i is a loop counter;
k is a number of blocks of p bits length into which A is divided;
$Y_0 = ((T.J_0) \bmod 2^p)$;
$J_0N = -1\text{mod}2^p$; and

Y_0 is calculated one bit at a time, based on the fact that $(T + NY_0)$ is a multiple of 2^p.

8. An apparatus for performing modular arithmetic, the apparatus comprising:

a first AND gate configured to receive first and second inputs and to generate a first output;

a second AND gate configured to receive third and fourth inputs and to generate a second output;

a divider configured to generate a third output;

a first carry-save adder configured to receive as inputs the first output from the first AND gate, the second output from the second AND gate, and the third output from the divider and to generate fourth and fifth outputs; and

a second carry-save adder configured to receive the combination of the fourth output and a fifth input as one input and to receive the fifth output as a second input and to generate a carry output that is fed back into a third input of the second carry-save adder and to generate a result output that is an input to the divider and the desired result.

9. The apparatus of claim 8, comprising a first register having the carry output of the second carry-save adder as an input and its output feeding back to the third input of the carry-save adder; and a second register receiving as an input the result and generating as an output the desired result that is fed back to the input of the divider and is the output of the apparatus.

10. The apparatus of claim 9, wherein the apparatus is configured to perform a modular operation of S = A.B mod N, where A, B and N are encoded as multi-bit digital words, including the following steps:

a) setting S(-1) to 0, and i to 0;

b) setting S(i) to $(S(i-1) + A<i>B + NY_0)/2^p$;

c) setting S(i) to (S(i) - N) if $S(i) \geq N$; and

d) repeating steps b) and c) k times;

wherein:

i is a loop counter;

k is a number of blocks of p bits length into which A is divided;

$Y_0 = ((T.J_0) \bmod 2^p)$;

J_0N = -1mod2^p; and

Y_0 is calculated one bit at a time, based on the fact that (T + NY_0) is a multiple of 2^p.

11. The apparatus of claim 10 wherein N is a prime number.

12. An apparatus for performing modular arithmetic, the apparatus comprising:

inputs A, B, and N, and an output S;

a first carry-save adder configured to receive five input signals, comprising:

U_0, the partial product of N and Y_0, where Y_0 equal ((T.J_0) mod 2^p);

U_1, the subtraction of a previous version of S and U_6, wherein U_6 is one of N or 0 depending on the value of a comparison between a result of a previous iteration and N;

U_2, a partial product of input B and a current version of input A;

U_3, the result of S/2; and

U_4, a carry output of a second carry-save adder;

the first carry-save adder configured to generate a result output and a carry output;

the second carry-save adder configured to receive the result output and the carry output from the first carry-save adder and to receive a compensation signal as a third input and to generate a desired result and the carry output U_4; and

wherein J_0N<0> = -1. mod 2^p, where p is a block length into which A is sub-divided.

13. The apparatus of claim 12 wherein the first carry-save adder is a two-stage carry-save adder.

14. The apparatus of claim 12 wherein the first carry-save adder comprises two one-stage carry-save adders arranged in series.

15. The apparatus of claim 12, comprising a register, an AND gate, and a multiplier configured to implement the compensation function in the event $t<p$ and the result output of the second carry-save adder = 1 the value N_{del} of the register is applied to the third input of the second carry-save adder, and when the condition is not satisfied, no compensation value is provided to the third input of the second carry-save adder.